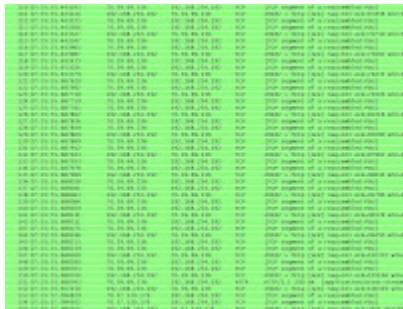


DarkMegie rootkit - sample (distributed via Blackhole)

Archived: 2026-04-05 17:29:22 UTC

Update April 20, 2012 Kimberly wrote an excellent analysis of this sample. Please go to

[Stopmalvertising](#) to read



This is a "DarkMegie" rootkit sample, kindly donated by Hendrik Adrian. Just like described in the McAfee article ["Darkmegie: This is Not the Rootkit You're Looking For" by Craig Schmugar](#), it is anything but quiet and stealthy.

In fact, it makes so many system changes that it is hard to cover it all in a quick post.

Indeed, it drops the rootkit components in drivers with the incredible padding to 25MB and generates a lot of traffic. Unfortunately, I did not have time yet to sort out the mess and purpose of all files that this malware creates so I am just posting it here along with sandbox results for you to analyze. If you write a detailed analysis, please share, I will link to.



Size: 77312

MD5: 6C8F9658A390C24A9F4551DC15063927



Download



[Download \(email me if you need the password scheme\)](#)

[Download the modified / created files and analysis data](#)

[Download pcap](#)

C:\Windows\System32\drivers\com32.sys

9728

4399b8a60977814197feae67c02a7ac2

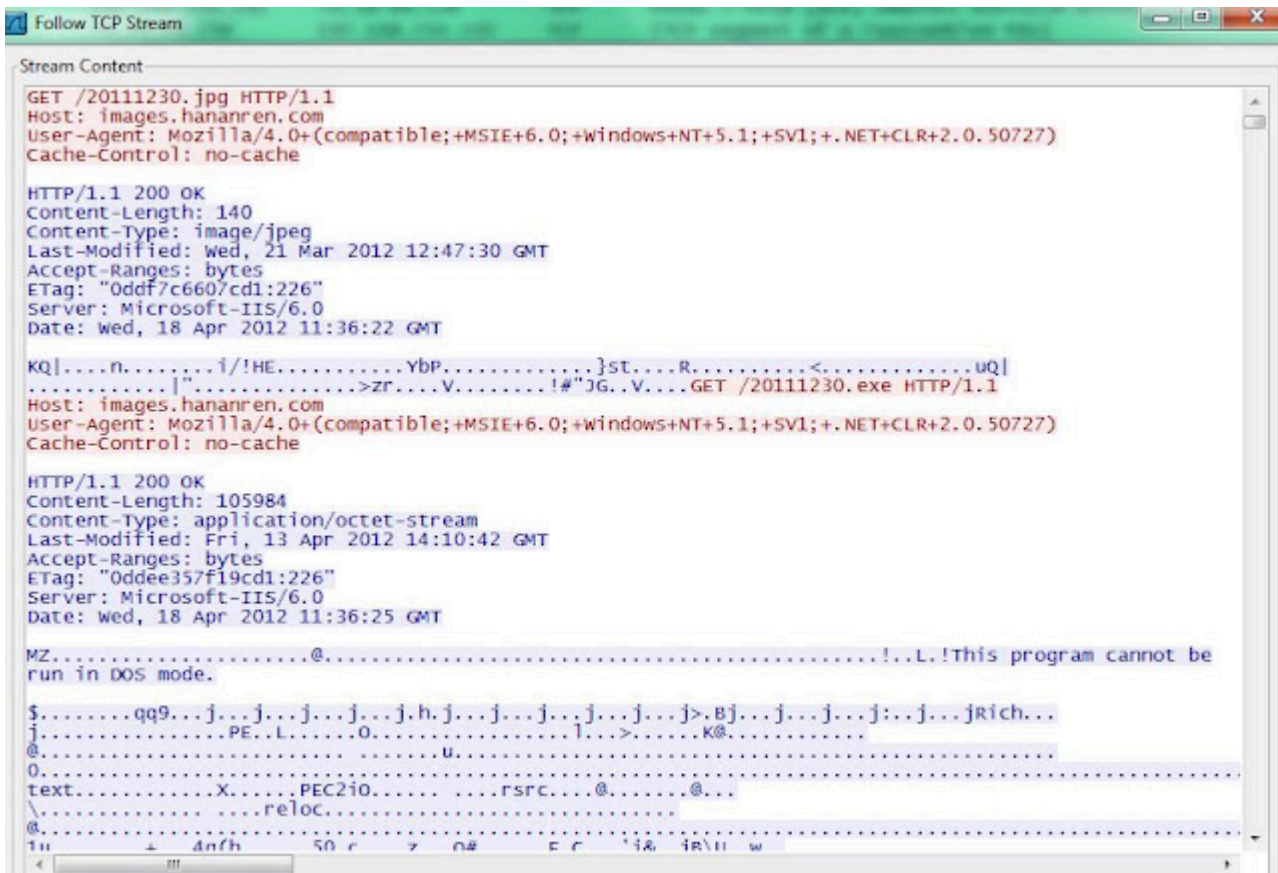
C:\Windows\System32\drivers\RCX50E3.tmp	26224256	9f32c51764f579512810b7ab3de1a91a
C:\Windows\System32\drivers\com32.sys	26224256	dd313b92f60bb66d3d613bc49c1ef35e
C:\Windows\System32\com32.dll	45056	25cfb72df8a30cbb7e6ee852bc31c50f
C:\Windows\System32\RCX5B11.tmp	31506432	2f00e0927c07bc44d9b79ccbe567f398
C:\Windows\System32\del043.bat	86	1a1e7855edc0afa6624080d60da8bf44

Traffic

It is as active as a click fraud or DDoS bot but does not fit these categories.

I am not quite sure what it is doing, please look and us know :)

5 07:35:51.164992	192.168.254.192	8.8.8.8	DNS	Standard query A images.hananren.com
6 07:35:51.179984	8.8.8.8	192.168.254.192	DNS	Standard query response A 70.39.69.236
7 07:35:51.439782	192.168.254.192	70.39.69.236	TCP	49182 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
8 07:35:51.673295	70.39.69.236	192.168.254.192	TCP	http > 49182 [SYN, ACK] Seq=0 Ack=1 Min=16384 Len=0 MSS=1460 WS=1 SACK_PERM=1
9 07:35:51.673423	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=1 Ack=1 win=65800 Len=0
10 07:35:51.706477	192.168.254.192	70.39.69.236	HTTP	GET /20111230.jpg HTTP/1.1
11 07:35:51.940349	70.39.69.236	192.168.254.192	HTTP	HTTP/1.1 200 OK (image/jpeg)
12 07:35:52.220243	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=172 Ack=366 Win=65432 Len=0
13 07:35:52.220243	192.168.254.192	70.39.69.236	TCP	[TCP Dup ACK 12#1] 49182 > http [ACK] Seq=172 Ack=366 Win=65432 Len=0
14 07:35:53.869212	192.168.254.192	8.8.8.8	DNS	Standard query A go.microsoft.com
15 07:35:53.878900	8.8.8.8	192.168.254.192	DNS	Standard query response CNAME www.go.microsoft.akadns.net A 64.4.11.25
16 07:35:54.014638	192.168.254.192	8.8.8.8	DNS	Standard query A images.hananren.com
17 07:35:54.035619	8.8.8.8	192.168.254.192	DNS	Standard query response A 70.39.69.236
18 07:35:54.039776	192.168.254.192	70.39.69.236	HTTP	GET /20111230.exe HTTP/1.1
19 07:35:54.271270	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
20 07:35:54.271378	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
21 07:35:54.271421	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=3238 Win=65800 Len=0
22 07:35:54.271692	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
23 07:35:54.468759	70.39.69.236	192.168.254.192	TCP	[TCP Dup ACK 22#1] http > 49182 [ACK] Seq=4674 Ack=343 Win=65193 Len=0
24 07:35:54.507567	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
25 07:35:54.507698	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=6110 Win=65800 Len=0
26 07:35:54.507747	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
27 07:35:54.507781	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
28 07:35:54.507809	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=8982 Win=65800 Len=0
29 07:35:54.658542	192.168.254.192	64.4.11.25	TCP	49181 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
30 07:35:54.681413	192.168.254.192	64.4.11.25	TCP	49184 > http [SYN] Seq=0 win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
31 07:35:54.740970	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
32 07:35:54.741086	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
33 07:35:54.741127	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=11854 Win=65800 Len=0
34 07:35:54.741450	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
35 07:35:54.741475	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
36 07:35:54.741496	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=14726 Win=65800 Len=0
37 07:35:54.741517	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
38 07:35:54.741748	70.39.69.236	192.168.254.192	TCP	[TCP segment of a reassembled PDU]
39 07:35:54.741772	192.168.254.192	70.39.69.236	TCP	49182 > http [ACK] Seq=343 Ack=17598 Win=65800 Len=0
40 07:35:54.753481	64.4.11.25	192.168.254.192	TCP	http > 49183 [SYN, ACK] Seq=0 Ack=1 Min=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
41 07:35:54.753563	192.168.254.192	64.4.11.25	TCP	49183 > http [ACK] Seq=1 Ack=1 win=65700 Len=0
42 07:35:54.754183	192.168.254.192	64.4.11.25	HTTP	GET /fwlink/?linkid=69157 HTTP/1.1
43 07:35:54.764884	64.4.11.25	192.168.254.192	TCP	http > 49184 [SYN, ACK] Seq=0 Ack=1 Min=8190 Len=0 MSS=1460 WS=16 SACK_PERM=1
44 07:35:54.764956	192.168.254.192	64.4.11.25	TCP	49184 > http [ACK] Seq=1 Ack=1 win=65700 Len=0
45 07:35:54.836830	64.4.11.25	192.168.254.192	HTTP	HTTP/1.1 302 Found (text/html)
46 07:35:54.848162	192.168.254.192	8.8.8.8	DNS	Standard query A www.msn.com
47 07:35:54.859978	8.8.8.8	192.168.254.192	DNS	Standard query response CNAME us.col.cb3.glbns.microsoft.com A 70.37.130.176



Some of the traffic

```
[process 8] 65.55.253.27 192.168.254.192 GET  
  
/c.gif?evt=br&rid=4571d83250544049bfc2ee88060f6bc8  
&exa=&cts=1334748967640&expac=&fk=W&gp=P&optkey=de  
fault&clid=23A3C63D37E16EEA2397C50633E16E45&cp=def  
ault&di=340&pi=7317&ps=95101&mk=en-us&pn=US+HPMSFT  
3Wdefault&pid=6901517&su=http%3A%2F%2Fwww.msn.com%  
2Fdefaultwpe3w.aspx&pageid=690151710&ce=1&hl=cplus  
&cm=head%3Ecb1
```

```
[process 8] 65.54.81.211 192.168.254.192 GET  
/i/87/DEC3F3D671E6CC76B09340612A38.jpg
```

```
[process 8] 207.46.193.176 192.168.254.192 GET  
  
/action/MSN_Homepage_Remessaging_111808/nc?a=1
```

```
[process 8] 207.46.193.176 192.168.254.192 none
```

```
[process 8] 208.44.23.25 192.168.254.192 none
```

```
[process 8] 208.44.23.25 192.168.254.192 GET
```

```
/b?c1=2&c2=3000001&c7=http%3A%2F%2Fwww.msn.com%2F%  
3Focid%3Diehp&c9=&rn=1334748958175
```

[process 8] 65.55.239.146 192.168.254.192 GET
/c.gif?udc=true&di=340&pi=7317&ps=95101&lng=en-us&
tp=http%3A%2F%2Fwww.msn.com%2Fdefaultwpe3w.aspx&ri
d=4571d83250544049bfc2ee88060f6bc8&rnd=13347489581
76&rf=&scr=1024x768

[process 8] 65.55.239.146 192.168.254.192 GET
/c.gif?udc=true&di=340&pi=7317&ps=95101&lng=en-us&
tp=http%3A%2F%2Fwww.msn.com%2Fdefaultwpe3w.aspx&ri
d=4571d83250544049bfc2ee88060f6bc8&rnd=13347489581
76&rf=&scr=1024x768&MUID=23A3C63D37E16EEA2397C5063
3E16E45&cb=1cd1d576b2f13a0

[process 8] 65.54.81.211 192.168.254.192 GET
/i/5E/4B835E56AC3C8535DB16275B4BAF4.jpg

[process 8] 65.54.80.242 192.168.254.192 GET
/i/BB/756A1C963A72E4AFBC36501B512725.jpg

[process 8] 65.54.81.211 192.168.254.192 GET
/i/E2/F757C6DFF15796123FA81CF7DCCF.jpg

[process 8] 65.55.239.146 192.168.254.192 GET
/c.gif?udc=true&di=340&pi=7317&ps=95101&lng=en-us&
tp=http%3A%2F%2Fwww.msn.com%2Fdefaultwpe3w.aspx&ri
d=4571d83250544049bfc2ee88060f6bc8&rnd=13347489581
76&rf=&scr=1024x768&RedC=c.msn.com&MXFR=23A3C63D37

E16EEA2397C50633E16E45

[process 8] 65.55.239.146 192.168.254.192 none

[process 8] 23.66.231.58 192.168.254.192 GET
/qsonhs.aspx?form=MSN005&q=

[process 8] 23.66.231.58 192.168.254.192 none

[process 8] 65.54.81.185 192.168.254.192 GET
/CIS/77/000/000/000/028/440.swf?fd=www.msn.com

[process 8] 65.54.81.185 192.168.254.192 GET
/CIS/18/000/000/000/024/175.jpg

Automatic scans

[Virusotal](#)

SHA256: a2c176ef3cc343194207e33acc19d5f8cb083a3c387a0404bd8f9d6bd29cfd6f

SHA1: c1af1fa6937097762824d0db039777ff35577727

MD5: 6c8f9658a390c24a9f4551dc15063927

File size: 75.5 KB (77312 bytes)

File name: DarkMegiSample

File type: Win32 EXE

Tags: yoda yodaprot

Detection ratio: 34 / 42

Analysis date: 2012-04-17 08:22:42 UTC (1 day, 3 hours ago)

More details

Antivirus Result Update

AhnLab-V3 Dropper/Rootkit.77312 20120417

AntiVir HEUR/Crypted 20120417

Antiy-AVL Trojan/Win32.Agent.gen 20120417

Avast Win32:Malware-gen 20120417

AVG PSW.Agent.ASED 20120417

BitDefender Trojan.Generic.KDV.503006 20120417

ByteHero - 20120417

CAT-QuickHeal TrojanSpy.Agent.bwtk 20120417

ClamAV PUA.Packed.YodaProt 20120417

Commtouch W32/Heuristic-210!Eldorado 20120417

Comodo TrojWare.Win32.TrojanDownloader.Agent.accn 20120417

DrWeb Trojan.PWS.Gamania.34539 20120417

Emsisoft Trojan.SuspectCRC!IK 20120417

eSafe Suspicious File 20120415

eTrust-Vet - 20120417

F-Prot W32/Heuristic-210!Eldorado 20120416

F-Secure Trojan.Generic.KDV.503006 20120417

Fortinet W32/Agent.BWTK!tr 20120417

GData Trojan.Generic.KDV.503006 20120417

Ikarus Trojan.SuspectCRC 20120417

Jiangmin TrojanSpy.Agent.uzc 20120417

K7AntiVirus Riskware 20120416

Kaspersky Trojan-Spy.Win32.Agent.bwtk 20120417

McAfee Artemis!6C8F9658A390 20120416

McAfee-GW-Edition - 20120417

Microsoft Trojan:Win32/Meredrop 20120417

NOD32 a variant of Win32/CsNowDown.C 20120417

Norman W32/Troj_Generic.ASBJ 20120416

nProtect Trojan/W32.Agent.77312.VC 20120417

Panda Generic Trojan 20120416

PCTools Downloader.Darkmegi 20120417

Sophos Mal/Packer 20120417

SUPERAntiSpyware - 20120402
Symantec Downloader.Darkmegi 20120417
TrendMicro Cryp_Yodap 20120417
TrendMicro-HouseCall Cryp_Yodap 20120417
VBA32 TrojanSpy.Agent.bwtk 20120416
VIPRE Trojan-Spy.Win32.Agent

Source: <http://contagiodump.blogspot.com/2012/04/this-is-darkmegie-rootkit-sample-kindly.html>